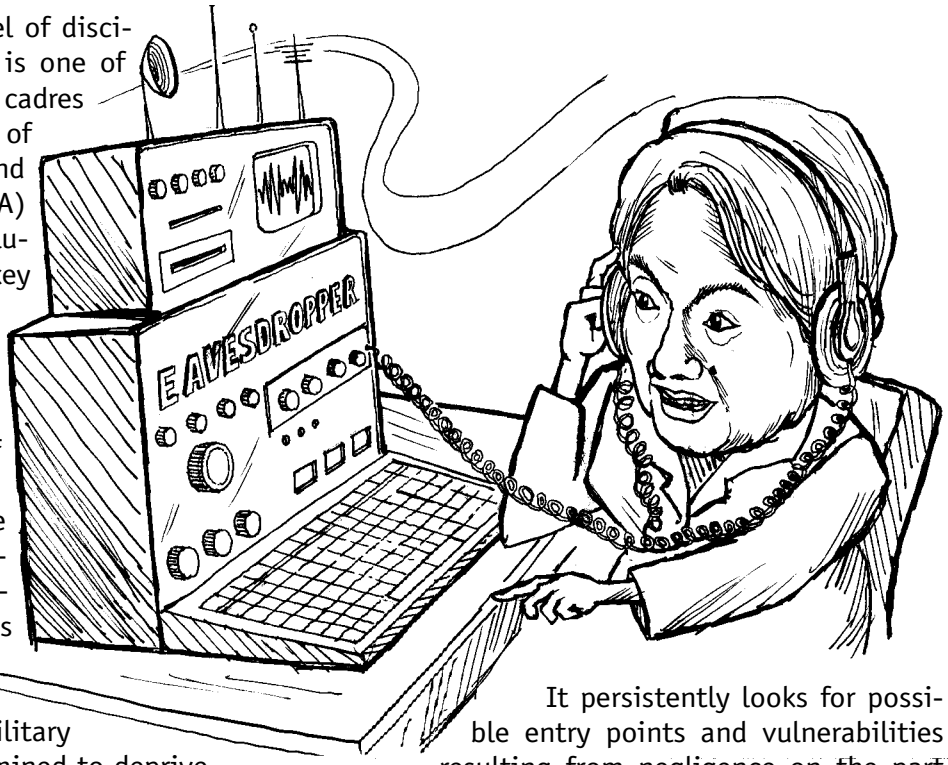
ANG Bayan
Pahayagan ng Partido Komunista ng Pilipinas
Pinapatnubayan ng Marxismo-Leninismo-Maoismo

Special Issue
English Edition
July 22, 2007
www.philippinerevolution.net

Keep the enemy deaf and blind

Excel in clandestine operations



The ability to exercise a high level of discipline in operating clandestinely is one of the most important qualities of cadres and members of the Communist Party of the Philippines (CPP), commanders and fighters of the New People's Army (NPA) and other elements within the revolutionary movement. It is one of the key factors behind the revolutionary movement's ability to preserve and strengthen its ranks, continue serving the people effectively and defeating the enemy one by one in the face of the latter's growing ferocity.

The revolutionary forces led by the CPP are constantly enhancing such discipline as well as their ability to conduct clandestine guerrilla operations that rely on the masses' deep and extensive support. In the face of the enemy's current superiority and military strength, the Party and NPA are determined to deprive him of the opportunity to inflict serious casualties on the revolutionary movement and the people.

Intensifying enemy surveillance operations. Under Operation Plan Bantay Laya 2 (OBL 2), the Arroyo regime and the Armed Forces of the Philippines (AFP) have been desperately trying to inflict the biggest damage possible on the revolutionary movement before the oplan's 2010 deadline. But we can deprive them of that pleasure if we can keep them blind and deaf regarding our current strength and the plans of the revolutionary forces as well as the actual location and movements of the Party, people's army and revolutionary underground movement.

The AFP has poured in a huge amount of funds and has gone all-out in intensifying its intelligence operations to gather information on Party organs, cadres and members; units and officers of the people's army; and leaders and members of mass organizations and their activities. It persistently looks for possible entry points and vulnerabilities resulting from negligence on the part of the revolutionary forces. It tirelessly awaits any opportunity for the revolutionary forces to breach discipline and commit errors in their movements so it could exploit the situation and launch precise and lethal attacks.

The AFP continues to set up intelligence networks and conduct physical surveillance, but these past several years, it has pulled all stops to raise its capability to conduct electronic surveillance through the use of modern equipment and technology. Currently, its main focus is on cellphone surveillance.

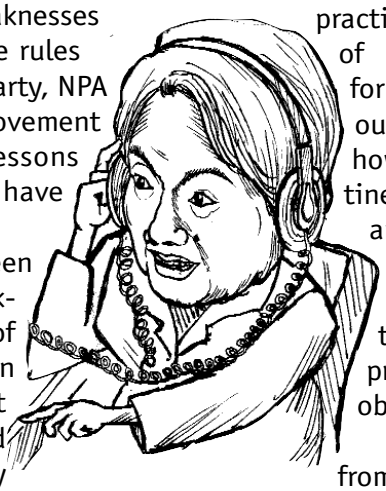
To pursue this, the Intelligence Service of the AFP (ISAFP) has formed MIG 21, a new branch specializing in this field. The various MIG units have been given equipment to intercept and monitor cellphone and landline communications in the cities and countryside. The Philippine National Police Intelligence Group (PNP-IG) and the government's other security agencies are engaged in parallel efforts. Simultaneously, other

units of the AFP, PNP and security agencies are enhancing their capabilities in other methods of surveillance.

The US also gives total support to the intelligence operations of the AFP, PNP and other security agencies. It provides training on intelligence work and gives or lends equipment. In addition, the US conducts its own intelligence operations by launching spy planes and conducting satellite surveillance and passes on gathered information to the AFP. It also enters the revolutionary movement's areas of operation for familiarization, to develop its own intelligence assets and undertake long-term intelligence work.

There are secret agreements between the AFP and cellphone companies allowing intelligence operatives to use certain pieces of company equipment to monitor identified cellphones. The ISAFP and PNP-IG likewise have in their possession modern surveillance equipment they have purchased, received from or borrowed from the US.

The enemy has, on occasion, inflicted casualties on the revolutionary forces due to the latter's negligence in observing security regulations and violation of the necessary tenets of operating clandestinely. There have been weaknesses in complying with the rules on discipline of the Party, NPA and underground movement and in applying lessons from past errors that have resulted in losses.



The enemy has been able to exploit weaknesses on the part of certain comrades in the way they contact their families and other persons already on the enemy's watchlist. There have also been weaknesses in the way sensitive documents and materials are kept and transferred. The most serious cases involve the careless use of electronic equipment, especially cellphones. There have likewise been many cases involving the reckless use of the internet and email.

Enhance our capability and intensify our efforts to operate clandestinely. The enemy's full-scale intelligence operations have made it even more important for the revolutionary forces to enhance their capability and intensify efforts to operate clandestinely. Such an endeavor hinges on the revolutionary forces' ability to strengthen their determination, patience and readiness for sacrifice, their willingness to apply iron discipline, conduct meticulous study and take the utmost care in everything they do and to take deep root among the masses.

All revolutionary forces must be mentally prepared to face necessary sacrifices and its attendant hardships. They must not rely excessively on things that are convenient but are likewise sources of vulnerabilities that could be exploited by the enemy.

We oblige Party cadres and members, NPA commanders and fighters and forces of the revolutionary underground movement to practice the highest levels of discipline. The need for everyone to continuously study and train on how to operate clandestinely, quietly, prudently and carefully is a must in dealing with sensitive matters where the strictest security precautions should be observed.

Everyone must learn from the guerrilla movements of the people's army that involve, among others, firm reliance on mass support; careful study and meticulous analysis of both our and the enemy's situation; maintaining the location of headquarters, points of origin and points of destination strictly confidential and hiking without leaving traces or tracks; and developing the ability to move and maneuver under cover of darkness.

Because of intensified electronic surveillance by the enemy, we put particular stress on avoiding vulnerabilities resulting from the use of cellphones. Everyone must have a basic understanding of the vulnerabilities and the extent to which the enemy can monitor cellphone conversations or text messages and pinpoint the location of cellphones under surveillance.

We must draft and develop a secure, effective and rapid system of communication that relies mainly on the depth of mass support. We must combine this with the selective, prudent, intelligent, planned and disciplined use of other systems of communication, both

Continued on "Editorial," on page 3

ANG Bayan
Special Issue July 22, 2007

Ang Bayan is published in Pilipino, Bisaya, Iloko, Hiligaynon, Waray and English editions.

It is available for downloading at the Philippine Revolution Web Central located at:

www.philippinerevolution.org

Ang Bayan welcomes contributions in the form of articles and news. Readers are likewise enjoined to send in their comments and suggestions for the betterment of our publication. You can reach us by email at:

angbayan@yahoo.com

Ang Bayan is published fortnightly by the Central Committee of the Communist Party of the Philippines

What is electronic surveillance?

Electronic surveillance involves monitoring electronic communications through the use of modern technology. Through electronic surveillance, agents of the state are able to monitor conversations over cellphones, landlines or radios, email and internet use. They can also determine the location of surveillance targets. Wiretapping, or listening in on landline or cellphone conversations is a form of electronic surveillance.

All forms of electronic surveillance are violative of the right to privacy of communications. Previously illegal, electronic surveillance has been legalized through the Human Security Act. Nonetheless, intelligence agencies of the reactionary state have long been extensively conducting electronic surveillance to monitor the people.

Particular targets of electronic surveillance are individuals and forces fighting the ruling regime who use electronic communications. Among them are activists, politicians, mass organizations and their headquarters, suspected cadres and forces of the Communist Party and people's army, as well as friends, relatives and sympathizers they come in contact with.

Information gathered from such sources is used by security agencies and the military in their counterrevolutionary war and campaigns of suppression, intimidation, killing and abduction.

Because such surveillance can be conducted surreptitiously and from afar, targets usually do not "feel" that they are being monitored. To avoid being caught in such a situation, we must meticulously study the vulnerabilities that accompany the use of modern communications equipment and come up with plans on how to prudently and wisely use such equipment.

What vulnerabilities arise with the use of cellphones?

A cellphone is, in essence, a two-way radio (like HF, VHF or UHF radios). Conversations and text messages travel through the air via radio signals. To be able to use a cellphone, there must be a cellsite nearby that will connect the cellphone in use with a telecommunications company's (like Smart, Globe and Sun) entire cellphone network .

A cellphone will connect to different cellsites, depending on the former's location. If there are several cellsites in the vicinity, the cellphone will connect to all of them. If there is no cellsite nearby, the cellphone will not be able to connect to the system and cannot be used for communication.

Because a cellphone continuously establishes connections with various cellsites, it can be easily used as a tracking device as long as it is on. A cellphone's relatively exact location can be determined through signal triangulation—especially in areas where there is more than one cellsite. Through signal triangulation, a cellphone's location may be determined by measuring the varying signal strengths received by the cellsites it has come in contact with.

Many of the newer model cellphones as well as other equipment have a Global Positioning System (GPS) installed. The locations of cellphones equipped with GPS can be determined both via satellite and through signal triangulation.

Cellphones can be easily monitored. First, cellphones identify themselves to cellsites and networks by transmitting information contained in their SIM (subscriber identification module) card. In addition, cellphones also transmit IMEI (International Mobile Equipment Identifier) and ESN (Electronic Serial Number) information. The IMEI and ESN are numbers embedded in cellphone parts. A cellphone's ESN can not be changed. Thus, once a cellphone has been pinpointed and monitored, it is virtually impossible for it and for all other cellphones it has come in contact with, to escape the "dragnet," even if the cellphone user changes its SIM and IMEI.

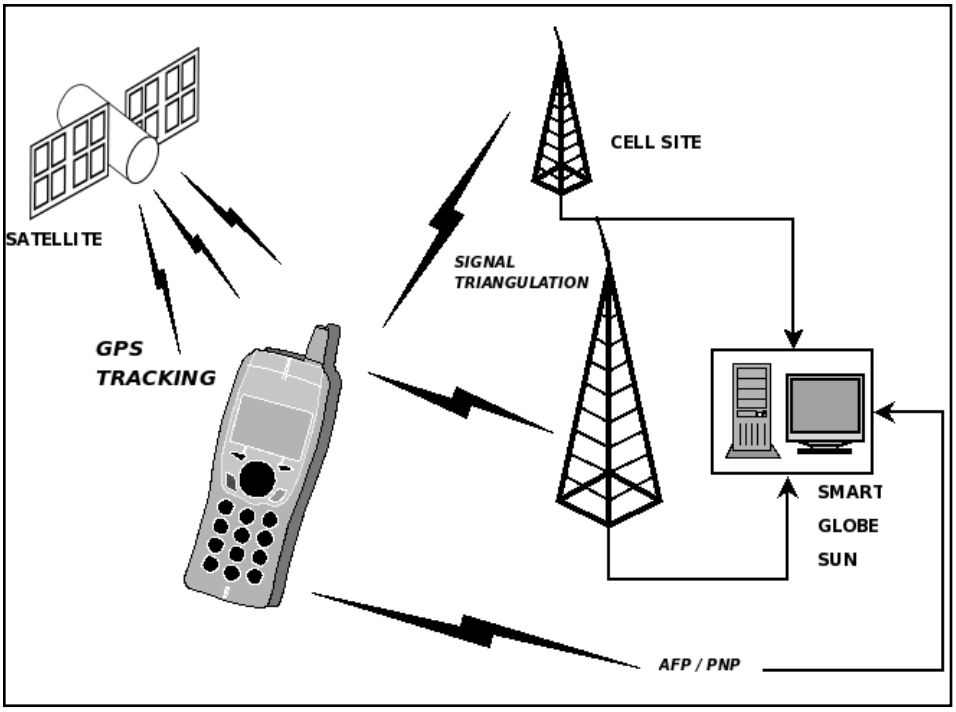
Text messages and conversations via cellphone can also be monitored using the facilities of cellphone companies. There are also short-range scanners/trackers for surveillance that function as transmitters between cellphone s and cellsites.

Stronger and more sophisticat-

"Editorial," from page 2

common or modern.

By practicing strict discipline, using guerrilla methods, relying on mass support and observing strict security measures in all our actions, we can avoid being pinpointed and ensnared by the enemy, even through electronic surveillance. Thus, we can render ineffective his millions of pesos worth of surveillance equipment. We can secure the Party, the people's army, the revolutionary movement and the masses' victories, avoid unnecessary major setbacks and ensure the revolution's continued advance. AB



ed scanners/trackers can be easily transported from place to place aboard a vehicle. The simpler ones can be easily carried by one person. These scanners/trackers can be used to monitor cellphones, determine their exact locations, listen in on conversations, read text messages, identify other cellphones they have connected to and determine the numbers of other cellphones in the immediate vicinity.

Cellphones equipped with "bluetooths" are even more vulnerable. Through the bluetooth, a portable computer can read all messages, all numbers listed in the address book and other information contained in a cellphone.

For as long as it is turned on, a monitored cellphone can also be used as a bugging device to intercept nearby conversations.

What vulnerabilities arise with the use of the internet?

The internet is the international system of interconnected computers. Through the internet, computers can exchange information even if they are thousands of kilometers apart. This system is usually used, among others, to exchange computer files and letters (email or electronic mail) and for calls.

For an email to be transmitted from one computer to another, the information contained therein must pass through various other computers within the international network. Thus, a message or file may be intercepted as it is transmitted from one computer to another and can easily be read by others if it is not ciphered.

Every piece of information passing through the internet contains identification regarding the computer it originated from. The main identification mark is the so-called "IP (or internet protocol) address," a number that is assigned to every computer connected to the internet. Using such information, the National Bureau of Investigation (NBI) was able to trace the house of the hacker who disseminated the "I love you virus" in 2000. The NBI was likewise able to trace the internet café used by the person who sent a statement taking responsibility for the burning of an ABS-CBN van in Pasig in 2005.

To intercept messages it considers or suspects to be contrary to US interests, the US Central Intelligence Agency launched a program under "Project Echelon" where internet messages containing key words such as "revolution," "communism," "movement," "imperialism" and the like are automatically detected. Such messages, as well as information on their points of origin and destination are collated for analysis.

Vulnerabilities can also arise from the use of internet cafés. Because computers in a café are part of a network, there are ways to monitor computer activity from a central computer. The café manager can monitor clients accessing particular websites (such as *www.philippinerevolution.net*).

Internet cafés also usually have closed circuit cameras as a precaution against criminals, but which can also be used for other purposes. Webcams attached to computers may also be used to take pictures of computer users. There are also military agents who roam inside internet cafés to observe clients and monitor persons who access websites maintained by the revolutionary movement and progressive organizations.

Computers that access the internet are likewise vulnerable to so-called viruses, trojans and other spyware. These are small computer programs that can read files or send information on the contents of a computer over the internet. Computers using the "Windows" operating system are particularly vulnerable because of the many security loopholes that can be taken advantage of by spyware makers. One can be infected by spyware by visiting certain websites, receiving email or even through USB drives connected to virus-infected computers in an internet café. AB